This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to items appearing in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Bugs, Holes, & Patches

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
ArGo Software Design ArGoSoft FTP Server 1.4.2.4 and prior	A vulnerability exists that could allow a remote user to determine valid usernames. A remote user can also conduct unlimited password guessing attempts. The vendor has issued a fixed version (1.4.2.1) to correct the username disclosure issue. No solution was available at the time of this entry for the unlimited password guessing issue. A Proof of Concept exploit has been published.	ArGoSoft FTP Server Discloses Username Status to Remote Users	Medium	SecurityTracker Alert ID: 1012744, December 31, 2004
Crystal Art Software Crystal FTP Pro 2.8	A buffer overflow vulnerability exists due to a boundary error in the handling of file extensions in response to 'LIST' requests, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. **A Proof of Concept exploit has been published.**	Crystal FTP Pro Buffer Overflow	High	Securiteam, December 19, 2004 **Packetstorm, December 31, 2004**
GFi MailEssentials 8.x, 9, 10.x	A denial of service vulnerability exists that could allow a remote user to stop GFI MailSecurity and GFI MailEssentials due to a bug in the Microsoft HTML parser library. A remote user can send a specially crafted HTML-based e-mail to trigger a flaw in the Microsoft HTML parser, causing GFI MailSecurity and GFI MailEssentials to stop processing. As a result, e-mail messages will be stuck in the Microsoft IIS or Exchange queues. A specially crafted javascript string in an e-mail subject, body, or attachment can trigger the crash. The vendor has issued the following fixes: GFI MailEssentials 10.x: ftp://ftp.gfi.com/patches/ME10_PATCH_20041220_01.zip GFI MailEssentials 9: ftp://ftp.gfi.com/patches/me9_PATCH_20041220_01.zip GFI MailSecurity 8.x: ftp://ftp.gfi.com/patches/MSEC8_PATCH_20041220_01.zip Currently we are not aware of any exploits for this vulnerability.	GFi MailEssentials Denial of Service Vulnerability CVE Name: CAN-2004-1312	Low	SecurityTracker Alert ID: 1012755, January 3, 2005
GlobalSCAPE, Inc. CuteFTP 6.0	Multiple buffer overflow vulnerabilities exist in the command and response functionality due to insufficient validation of user-supplied strings prior to copying them into finite process buffers, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. No workaround or patch available at time of publishing. **A Proof of Concept exploit has been published.**	GlobalScape CuteFTP Multiple Command Response Buffer Overflow	Low/ High (High if arbitrary code can be executed)	SecurityTracker Alert ID, 1012366, November 30, 2004 **Packetstorm, December 31, 2004**
Macallan Macallan Mail Solution 4.0.6.8 (Build 786)	A denial of service vulnerability exists that could allow a remote user to crash the web and POP3 services. A remote user can supply a specially crafted URL that begins with a question mark to cause the target service to crash. The vendor has issued a fixed version (4.1.1.0) at: macallan.club.fr/MMS/index.html A Proof of Concept exploit has been published.	Macallan Mail Solution Denial of Service Vulnerability	Low	CIRT Security Advisory, December 31, 2004
Microsoft Internet Explorer (Windows XP with SP2 is not affected)	A vulnerability exists due to an input validation error in the handling of FTP file transfers. This can be exploited by a malicious FTP server to create files in arbitrary locations via directory traversal attacks by tricking a user into downloading malicious files (e.g. by dragging or copying a file or folder). No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Internet Explorer FTP Download Directory Traversal	High	Secunia, SA13704, January 3, 2005

Microsoft Windows NT Server 4.0 SP 6a, NT Server 4.0 Terminal Server Edition SP 6, Windows 2000 Server SP 3 & SP4, Windows Server 2003, 2003 64-Bit Edition	A vulnerability exists due to an unchecked buffer in the handling of the 'Name' parameter from certain packets, which could let a remote malicious user execute arbitrary code. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-045.mspx **A Proof of Concept exploit has been published.**	Microsoft WINS Name Validation CVE Name: CAN-2004-0567	High	Microsoft Security Bulletin, SB04-045, December 14, 2004 US-CERT Vulnerability Note, VU#378160, December 16, 2004 **Packetstorm, January 2, 2005**
Microsoft Windows NT Server 4.0, Windows NT Server 4.0 Enterprise Edition, Windows NT Server 4.0 Terminal Server Edition, Windows 2000 Advanced Server, Windows 2000 Datacenter Server, Windows 2000 Professional, Windows 2000 Server, Windows XP Home Edition, Windows XP Professional, Windows Server 2003 Datacenter Edition, Windows Server 2003 Enterprise Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Web Edition, Windows 98, Windows 98 SE, Windows ME; **Avaya DefinityOne Media Servers, IP600 Media Servers, Modular Messaging (MSS) 1.1, (MSS) 2.0, S3400 Message Application Server,** **S8100 Media Servers**	A remote code execution vulnerability exists in the NetDDE services because of an unchecked buffer. A malicious user who successfully exploited this vulnerability could take complete control of an affected system. However, the NetDDE services are not started by default and would have to be manually started for an attacker to attempt to remotely exploit this vulnerability. This vulnerability could also be used to attempt to perform a local elevation of privileges or remote Denial of Service. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-031.mspx Avaya: Customers are advised to follow Microsoft's guidance for applying patches. Please see the referenced Avaya advisory at the following location for further details: http://support.avaya.com/japple/css/japple?temp.groupID=128450&temp.selectedFamily=128451&temp.selectedProduct=154235&temp.selectedBucket=126655&temp.feedbackState=askForFeedback&temp.documentID=203487&PAGE=avaya.css.CSSLvl1Detail&executeTransaction=avaya.css.UsageUpdate() **A Proof of Concept exploit has been published.**	Microsoft NetDDE Remote Code Execution CVE Name: CAN-2004-0206	High	Microsoft Security Bulletin MS04-031, October 12, 2004 US-CERT Cyber Security Alert SA04-286A, October 12, 2004 US-CERT Vulnerability Note VU#640488, October 13, 2004 SecurityFocus, October 18, 2004 **Packetstorm, January 2, 2005**
Mozilla Bugzilla 2.x	A vulnerability exists which can be exploited by malicious people to conduct cross-site scripting attacks. Input passed in HTTP requests is not properly sanitized before being returned to users in error messages when an internal error is encountered. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site. Fixes are reportedly available in the CVS repository. Currently we are not aware of any exploits for this vulnerability.	Mozilla Bugzilla Internal Error	High	Bugzilla Bug 272620, January 3, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Benchmark Designs Project WHM AutoPilot	Several vulnerabilities were reported in WHM AutoPilot. A remote user can execute arbitrary commands on the target system, conduct cross-site scripting attacks, or obtain information about the target system. Several scripts do not properly validate user-supplied input. A remote user can load several scripts and supply a specially crafted 'server_inc' value to cause the script to include and execute arbitrary PHP code. The PHP code, including operating system commands, will run with the privileges of the target web service. The vendor has issued a fixed version: www.whmautopilot.com/index.php A Proof of Concept exploit has been published.	Benchmark Designs WHM AutoPilot 'server_inc' Include File Flaw	High	GulfTech Security Advisory, December 27, 2004
Conectiva Conectiva Linux 9 - netpbm	A vulnerability exist in netpbm which can be exploited by malicious, local users to escalate their privileges on a vulnerable system. The vulnerability is caused due to insecure creation of temporary files, which can be exploited via symlink attacks. Apply updated packages: http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000909 Currently we are not aware of any exploits for this vulnerability.	Conectiva netpbm Privilege Escalation	Medium	Secunia, SA13682, December 30, 2004

GNU CUPS 1.x	A vulnerability has been reported in CUPS, which potentially can be exploited by malicious people to compromise a vulnerable system. Successful exploitation may potentially allow execution of arbitrary code with the privileges of the print spooler, when a specially crafted PDF document is printed. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates Gentoo: http://security.gentoo.org/glsa/glsa-200412-25.xml **Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:164** **Debian: http://www.debian.org/security/2004/dsa-621** Currently we are not aware of any exploits for this vulnerability.	GNU CUPS xpdf "doImage()" Buffer Overflow Vulnerability	High	Secunia SA13668, December 26, 2004 **Mandrakesoft, MDKSA-2004:164, December 29, 2004**
GNU CVSTrac 1.x	Vulnerabilities exist due to a lack of input validation in "main.c" and "login.c". This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site. Update to version 1.1.5: http://www.cvstrac.org/cvstrac/wiki?p=DownloadCvstrac Currently we are not aware of any exploits for this vulnerability.	GNU CVSTrac Cross-Site Scripting Vulnerabilities	High	CVSTrac, Check in Numbers 320, 321, December 17, 2004
GNU Xpdf prior to 3.00pl2	A buffer overflow vulnerability exists that could allow a remote user to execute arbitrary code on the target user's system. A remote user can create a specially crafted PDF file that, when viewed by the target user, will trigger an overflow and execute arbitrary code with the privileges of the target user. A fixed version (3.00pl2) is available at: http://www.foolabs.com/xpdf/download.html A patch is available: ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.00pl2.patch KDE: http://www.kde.org/info/security/advisory-20041223-1.txt Gentoo: http://security.gentoo.org/glsa/glsa-200412-24.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/ **Mandrakesoft (update for koffice): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:165** **Mandrakesoft (update for kdegraphics): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:163** **Mandrakesoft (update for gpdf): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:162** **Mandrakesoft (update for xpdf): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:161** **Mandrakesoft (update for tetex): http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:166** **Debian: http://www.debian.org/security/2004/dsa-619** **Fedora (update for tetex): http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** Currently we are not aware of any exploits for this vulnerability.	GNU Xpdf Buffer Overflow in doImage() CVE Name: CAN-2004-1125	High	iDEFENSE Security Advisory 12.21.04 KDE Security Advisory, December 23, 2004 **Mandrakesoft, MDKSA-2004:161,162,163,165, 166, December 29, 2004**

IBM AIX 5.x	Multiple vulnerabilities exist in AIX, which can be exploited by malicious, local users to gain escalated privileges. These vulnerabilities exist in the 'paginit' utility, the '/bin/Dctrl' utility, the 'uname' utility, and the 'grep' utility. Successful exploitation of the vulnerabilities allows execution of arbitrary code with 'root' privileges. Apply APARs: http://www-912.ibm.com/eserver/support/fixes/fcgui.jsp **A Proof of Concept exploit has been published.**	IBM AIX Multiple Privilege Escalation Vulnerabilities	High	iDEFENSE Security Advisory 12.20.04 **Packetstorm, December 31, 2004**
KDE KDE 3.x, 2.x	A vulnerability exists in kio_ftp, which can be exploited by malicious people to conduct FTP command injection attacks. The vulnerability has been fixed in the CVS repository. Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:160 Currently we are not aware of any exploits for this vulnerability.	KDE kio_ftp FTP Command Injection Vulnerability	Medium	KDE Advisory Bug 95825, December 26, 2004
Multiple Vendors Linux Kernel 2.4 - 2.4.28, 2.6 - 2.6.9	A vulnerability was reported in the Linux kernel in the auxiliary message (scm) layer. A local malicious user can cause Denial of Service conditions. A local user can send a specially crafted auxiliary message to a socket to trigger a deadlock condition in the __scm_send() function. **Ubuntu: http://security.ubuntu.com/ubuntu/pool/** **SUSE: http://www.novell.com/linux/security/advisories/2004_44_kernel.html** **Trustix: http://http.trustix.org/pub/trustix/updates/** **Red Hat: http://rhn.redhat.com/errata/RHSA-2004-689.html** **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** A Proof of Concept exploit script has been published.	Multiple Vendors Linux Kernel Auxiliary Message Layer State Error CVE Name: CAN-2004-1016	Low	iSEC Security Research Advisory 0019, December 14, 2004 **SecurityFocus, December 25, 2004** **Secunia, SA13706, January 4, 2005**
Multiple Vendors Linux Kernel 2.4 - 2.4.28, 2.6 - 2.6.9	Several vulnerabilities exist in the Linux kernel in the processing of IGMP messages. A local user may be able to gain elevated privileges. A remote user can cause the target system to crash. These are due to flaws in the ip_mc_source() and igmp_marksources() functions. **SUSE: http://www.novell.com/linux/security/advisories/2004_44_kernel.html** **Trustix: http://http.trustix.org/pub/trustix/updates/** **Ubuntu: http://security.ubuntu.com/ubuntu/pool** **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** A Proof of Concept exploit script has been published.	Multiple Vendors Linux Kernel IGMP Integer Underflow CVE Name: CAN-2004-1137	Low/ Medium (Medium if elevated privileges can be obtained)	iSEC Security Research Advisory 0018, December 14, 2004 **SecurityFocus, December 25, 2005** **Secunia, SA13706, January 4, 2005**
Multiple Vendors **Linux Kernel 2.6.x**	Some potential vulnerabilities exist with an unknown impact in the Linux Kernel. The vulnerabilities are caused due to boundary errors within the 'sys32_ni_syscall()' and 'sys32_vm86_warning()' functions and can be exploited to cause buffer overflows. Immediate consequences of exploitation of this vulnerability could be a kernel panic. It is not currently known whether this vulnerability may be leveraged to provide for execution of arbitrary code. Patches are available at: http://linux.bkbits.net:8080/linux-2.6/cset@1.2079 http://linux.bkbits.net:8080/linux-2.6/gnupatch@41ae6af1cR3mJYlW6D8EHxCKSxuJiQ **Ubuntu: http://security.ubuntu.com/ubuntu/pool/** **SUSE: http://www.novell.com/linux/security/advisories/2004_44_kernel.html** **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** Currently we are not aware of any exploits for these vulnerabilities.	Multiple Vendors Linux Kernel 'sys32_ni_syscall' and 'sys32_vm86_warning' Buffer Overflows CVE Name: CAN-2004-1151	Low/High (High if arbitrary code can be executed)	Secunia Advisory ID, SA13410, December 9, 2004 SecurityFocus, December 14, 2004 **SecurityFocus, December 25, 2004** **Secunia, SA13706, January 4, 2005**
Multiple Vendors perl	Multiple vulnerabilities exist which can be exploited by malicious, local users to perform certain actions on a vulnerable system with escalated privileges. A local attacker could create symbolic links in the temporary files directory, pointing to a valid file somewhere on the file system. When a Perl script is executed, this would result in the file being overwritten with the rights of the	Multiple Vendors Perl Insecure Temporary File Creation	Medium	Gentoo Security Advisory, GLSA 200412-04 / perl, December 7, 2004 Trustix Secure Linux Bugfix

	user running the utility, which could be the root user. Gentoo: update to "perl-5.8.5-r2" or later: http://security.gentoo.org/glsa/glsa-200412-04.xml Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/p/perl/ **Debian: http://www.debian.org/security/2004/dsa-620** Currently we are not aware of any exploits for these vulnerabilities.			Advisory #2004-0050, November 30, 2004 Ubuntu Security Notice USN-16-1 November 02, 2004 **Debian DSA-620-1 perl, December 30, 2004**
Multiple Vendors glibc 2.2	A buffer overflow vulnerability exists in the resolver libraries of glibc 2.2. SUSE: ftp://ftp.SUSE.com/pub/SUSE Red Hat: http://rhn.redhat.com/errata/RHSA-2004-586.html **Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:159** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors glibc Buffer Overflow CVE Name: CAN-2002-0029 **CAN-2004-0968**	Low	SUSE Security Summary Report, SUSE-SR:2004:002, November 30, 2004 Red Hat RHSA-2004:586-15, December 20, 2004 **Mandrakesoft, MDKSA-2004:159, December 29, 2004**
MySQL Eventum 1.3.1	Multiple vulnerabilities exist which can be exploited by malicious people to conduct cross-site scripting and script insertion attacks and potentially bypass certain security restrictions. 1) Input passed to the "email" parameter in "index.php" and"forgot_password.php", and the "title" and "outgoing_sender_name" parameters in "projects.php" is not properly sanitized before being returned to users. 2) Input passed to the "full_name", "sms_email", "list_refresh_rate", and "emails_refresh_rate" parameters in "preferences.php" is not properly sanitized 3) Eventum has a undocumented default administrator account. No vendor solution is available. Currently we are not aware of any exploits for this vulnerability.	MySQL Eventum Multiple Vulnerabilities	High	CIRT-200404 and CIRT-200405: December 28, 2004
Nullsoft SHOUTcast 1.9.4	A format string vulnerability exists that could allow a remote user to execute arbitrary code on the target system. A remote user can supply a specially crafted request to the target server containing format string characters to cause the target service to crash or execute arbitrary code. No workaround or patch available at time of publishing. **A Proof of Concept exploit has been published.**	Nullsoft SHOUTcast Format String Flaw	High	SecurityTracker Alert ID: 1012675, December 24, 2004 **Packetstorm, December 31, 2004**
phpBB Group phpBB 2.0.0-2.0.10	A vulnerability exists in the 'urldecode' function due to insufficient input validation, which could let a remote malicious user execute arbitrary PHP script. No workaround or patch available at time of publishing. **Additional exploit scripts have been published.**	PHPBB Remote URLDecode Input Validation	High	Bugtraq, November 13, 2004 SecurityFocus, November 23, 2004 **SecurityFocus December 25, 2004**
Toshiaki Kanosue HtmlHeadLine.sh	A vulnerability exists due to multiple temporary files being created insecurely. This can be exploited via symlink attacks to overwrite arbitrary files with the privileges of the user running the vulnerable script. Debian: http://www.debian.org/security/2005/dsa-622 Currently we are not aware of any exploits for this vulnerability.	Toshiaki Kanosue HtmlHeadLine.sh Insecure Temporary File Creation	Medium	Secunia, SA13714, January 3, 2005

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
Albrecht Günther PHProjekt 4.x	A vulnerability exists in PHProjekt, which can be exploited by malicious people to compromise a vulnerable system. Input passed to the "path_pre" parameter in "authform.inc.php" isn't properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources. The vulnerability has been fixed in version 4.2.3. Apply patch for version 4.2: http://www.phprojekt.com/files/4.2/lib.zip **Gentoo:** **http://security.gentoo.org/glsa/glsa-200412-27.xml** Currently we are not aware of any exploits for this vulnerability.	Albrecht Günther PHProjekt "path_pre" Parameter Arbitrary File Inclusion Vulnerability	High	PHProjekt Security Advisory, December 28, 2004 **Gentoo, GLSA 200412-27, December 30, 2004**

All Enthusiast, Inc. PhotoPost PHP Pro 4.x	Multiple vulnerabilities exist which can be exploited by malicious people to conduct cross-site scripting and SQL injection attacks. 1) Input passed to the "page", "cat", and "si" parameters in "showgallery.php" isn't properly sanitized before being returned to the user. 2) Input passed to the "cat" and "ppuser" parameters in "showgallery.php" isn't sanitized properly before being used in a SQL query. Update to version 4.86: http://www.photopost.com/ Currently we are not aware of any exploits for this vulnerability.	All Enthusiast PhotoPost PHP Pro Cross-Site Scripting and SQL Injection	High	GulfTech Security Research Team, January 3, 2005
All Enthusiast, Inc. ReviewPost PHP Pro 2.x	Multiple vulnerabilities exist which can be exploited by malicious people to conduct cross-site scripting and SQL injection attacks, and compromise a vulnerable system. 1) Input passed to the "si" parameter in "showcat.php", "cat" and "page" parameters in "showproduct.php", and "report" parameter in "reportproduct.php" isn't properly sanitized before being returned to the user. 2) Input passed to the "cat" parameter in "showcat.php" and "product" parameter in "addfav.php" isn't properly sanitized before being used in a SQL query. 3) An error in the handling of file uploads for filenames with multiple extensions (e.g. "test.jpg.php.jpg.php") can be exploited. Update to version 2.84: http://www.photopost.com/ Currently we are not aware of any exploits for this vulnerability.	All Enthusiast ReviewPost PHP Pro Multiple Vulnerabilities	High	GulfTech Security Research Team, January 3, 2005
Ben3W 2Bgal 2.4 and 2.5.1	A vulnerability exists that can be exploited by malicious people to conduct SQL injection attacks. Input passed to the "id_album" parameter is not properly sanitized before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code. No workaround or patch available at time of publishing. **A Proof of Concept exploit has been published.**	Ben3W 2Bgal "id_album" SQL Injection Vulnerability	High	Secunia SA13620, December 23, 2004 **Packetstorm, December 31, 2004**
Colin Stéphane aStats 1.6.5	A vulnerability exists which can be exploited by malicious, local users to perform certain actions on a vulnerable system with escalated privileges. The vulnerability is caused due to the astats script creating some PNG images and the aStats-Graphic-Signature-Generation file insecurely. This can be exploited via symlink attacks to overwrite arbitrary files with the privileges of the user running the vulnerable script. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Colin Stéphane aStats Insecure Temporary File Creation	Medium	Secunia, SA13679, December 29, 2004
GForge Limbo 1.0.2	Multiple vulnerabilities exist which can be exploited by malicious people to conduct cross-site scripting and script insertion attacks, and potentially compromise a vulnerable system. 1) Input passed to the "searchword" parameter in "index.php" isn't properly sanitized before being returned to the user. 2) Input passed to "gb_name", "gb_email", "gb_url", "gb_country", "gb_title", and "gb_message" is not properly sanitized before being used. The vulnerabilities have been fixed in version 1.0.3 alpha. A Proof of Concept exploit has been published.	GForge Limbo Multiple Vulnerabilities	High	TheBillyGoatCurse.com, December 27, 2004
Glandrake.com MyCart	A vulnerability exists that could permit a remote user to view the configuration file. A remote user can directly request the 'settings.ini' file, which includes database passwords and other potentially sensitive system information. A fixed version (version as of March 19, 2001) is available at: http://glandrake.com/scripts/php/rosenet/mod2_cart.tgz A Proof of Concept exploit has been published.	Glandrake.com MyCart Discloses Configuration File	Medium	SecurityTracker Alert ID: 1012752, January 3, 2005
GNU FlatNuke 2.5.1	A vulnerability exists in which a remote user can gain administrative access on the application. A remote user can also execute arbitrary PHP code on the target system. The 'index.php' script does not properly validate user-supplied input in the 'url_avatar' field. A remote user can submit a specially crafted value to register as an administrative user. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	GNU FlatNuke Input Validation Flaw in 'url_avatar'	High	SecurityTracker Alert ID: 1012758, January 3, 2005
GNU Moodle 1.4.2 and prior versions	Multiple vulnerabilities exist that could permit a remote user to obtain session ID files. A remote user can also conduct cross-site scripting attacks. The '/mod/forum/view.php' script does not properly validate user-supplied input in the $search variable. Also, a remote user can invoke 'file.php' to obtain session data stored in the 'moodledata' directory. The 'pathname' variable is not properly validated. The session file disclosure vulnerability was patched on December 14, 2004 in version 1.4.3. No solution was available at the time of this entry for the cross-site scripting vulnerabilities, but a fix is planned (potentially for the future version 1.5). A Proof of Concept exploit has been published.	GNU Moodle Input Validation Vulnerability	High	SecurityTracker Alert ID: 1012710, December 28, 2004
GNU Owl Intranet Engine prior to 0.74.0	An input validation vulnerability exists in the Owl intranet engine that could permit a remote user to conduct cross-site scripting attacks and SQL injection attacks. A remote user can also cause arbitrary scripting code to be executed by the target user's browser.	GNU Owl Intranet Engine Input Validation Holes	High	Nessus Reference: 16063

	No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.			
GNU PHP-Calendar	A vulnerability exists that could allow a remote user to execute arbitrary commands on the target system. The software does not properly validate user-supplied input in the 'phpc_root_path' variable. If the php globals configuration is set, then a remote user can supply a specially crafted URL to cause arbitrary PHP code from a remote site to be included and executed by the target system. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	GNU PHP-Calendar Include File Flaw	High	GulfTech Security Advisory, December 29, 2004
GNU ViewCVS 0.9.2	Multiple vulnerabilities exist that could allow a remote user to conduct cross-site scripting attacks. The 'viewcvs.py' script does not properly validate user-supplied input in the 'content-type' and the 'content-length' parameters. A remote user can create a specially craft URL that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	GNU ViewCVS Input Validation Holes	High	SecurityTracker Alert ID: 1012750, January 2, 2005
Google Gmail	A vulnerability exists that could allow a remote user to send a large amount of e-mail to the target user's secondary address. The Gmail service 'forgot your password?' feature allows a remote user to load a certain URL to cause the service to send a validation e-mail to the specified user's secondary e-mail address. There is no limit to the number of messages sent over a period of time, so a remote user can flood the target user's secondary e-mail address. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Google Gmail 'forgot your password?' Vulnerability	Low	SecurityTracker Alert ID: 1012749, January 2, 2005
GRASS Development Team GRASS 5.7.x	Multiple vulnerabilities exist which can be exploited by malicious, local users to perform certain actions on a vulnerable system with escalated privileges. The vulnerabilities are caused due to multiple scripts creating temporary files insecurely. This can be exploited via symlink attacks to overwrite arbitrary files with the privileges of the user running a vulnerable script. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	GRASS Multiple Scripts Insecure Temporary File Creation	Medium	Debian Bug #287651, December 29, 2004
Joe Lumbroso Jack's FormMail.php 5.0	A vulnerability exists that could allow a remote user to view files on the target system. A remote user can specify a value for the 'ar_file' auto-reply parameter to cause the target server to send an arbitrary file to the remote user. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Joe Lumbroso Jack's FormMail.php File Access Vulnerability	Medium	SecurityTracker Alert ID: 1012747, January 1, 2005
korWeblog 1.6.2-cvs and prior versions	Multiple input validation vulnerabilities exist that could allow a remote user to execute arbitrary commands on the target system. The '/install/index.php' script does not properly validate the user-supplied 'lng' parameter. A remote user can create a specially crafted URL to cause the target server to include and execute arbitrary PHP code located on a remote server. A remote user can also view files on the target system. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	KorWeblog 'install/index.php' Include File Flaw	High	SecurityTracker Alert ID: 1012745, January 1, 2005
Mozilla Mozilla 1.7.3	A heap overflow vulnerability exists in the processing of NNTP URLs. A remote user can execute arbitrary code on the target system. A remote user can create a specially crafted 'news://' URL that, when loaded by the target user, will trigger a buffer overflow and execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The flaw resides in the *MSG_UnEscapeSearchUrl() function in 'nsNNTPProtocol.cpp'. The vendor has issued a fixed version (1.7.5), available at: http://www.mozilla.org/products/mozilla1.x/ A Proof of Concept exploit has been published.	Mozilla Buffer Overflow in Processing NNTP URLs	High	iSEC Security ResearchAdvisory, December 29, 2004
Mozilla Mozilla 1.7.3 for Linux, Mozilla 1.7.5 for Windows, and Mozilla Firefox 1.0	A vulnerability exists which can be exploited by malicious people to spoof the source displayed in the Download Dialog box. The problem is that long sub-domains and paths aren't displayed correctly, which therefore can be exploited to obfuscate what is being displayed in the source field of the Download Dialog box. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Mozilla / Mozilla Firefox Download Dialog Source Spoofing	Medium	Secunia SA13599, January 4, 2005
QNX Software Systems QNX RTOS 2.4, 4.25, 6.1.0, 6.2.0 (+ Update Patch A)	A vulnerability exists in the QNX operating system in crttrap. A local user can read and write arbitrary files on the target system. A local user can invoke crttrap with the '-c' command option and the 'trap' flag to write a trap file to an arbitrary location with root privileges. No workaround or patch available at time of publishing.	QNX crttrap '-c' Lets Local Users Read or Write Arbitrary Files	High	SecurityTracker Alert ID: 1012712, December 29, 2004

	A Proof of Concept exploit has been published.			
Simon Tatham PuTTY for Symbian OS 1.x	A vulnerability exists which potentially can be exploited by malicious people to compromise a user's system. The vulnerability has been fixed in version 1.3.2 RC1P: http://s2putty.sourceforge.net/ Currently we are not aware of any exploits for this vulnerability.	Simon Tatham PuTTY for Symbian OS "SSH2_MSG_DEBUG" Buffer Overflow	Unknown	Secunia, SA13678, January 4, 2005
SIR GNUBoard 3.40 and prior version	An input validation vulnerability exists that could allow a remote user with file upload privileges to upload arbitrary scripting code to the target system. The 'gbupdate.php' script does not properly validate the file extensions of uploaded files, performing only a case-sensitive check. A remote user can upload files containing scripting code and having a file extension commonly associated with scripting files (e.g., php, pl, cgi). Then, the remote user can cause the web server to execute the uploaded file. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	SIR GNUBoard Case-Sensitive File Extension Validation Vulnerability	High	STG Security, January 2005
Symantec Symantec Nexland Firewall Appliances 1.x	Three vulnerabilities exist in the Nexland Firewall Appliances, which can be exploited by malicious people to cause a DoS (Denial of Service), identify active services, and manipulate the firewall configuration. Update to firmware build 16U: http://www.symantec.com/techsupp/ Currently we are not aware of any exploits for this vulnerability.	Symantec Nexland Firewall Appliances Vulnerabilities	Medium	Symantec Advisory, SYM04-013, December 28, 2004
ViewCVS ViewCVS 0.9.2 & prior	A vulnerability exists because it is possible to access CVSROOT and forbidden directories via the tarball generation functionality, which could let malicious user bypass security restrictions. Debian: http://security.debian.org/pool/updates/main/v/viewcvs/ **Gentoo: http://security.gentoo.org/glsa/glsa-200412-26.xml** A Proof of Concept exploit has been published.	ViewCVS Ignores 'hide_cvsroot' and 'forbidden' Settings	Medium	SecurityTracker Alert ID, 1012431, December 6, 2004 **Gentoo Advisory GLSA 200412-26, December 28, 2004**
Xanga.com Xanga	An input validation vulnerability exists that could allow a remote user to conduct cross-site scripting attacks. 'sitemessage.aspx' does not properly validate user-supplied input. A remote user can create a specially crafted URL that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Xanga 'sitemessage.aspx' Input Validation Flaw	High	SecurityTracker Alert ID: 1012751, January 2, 2005
ZyXEL B-240 Wireless Ethernet Adapter	A remote cross-site scripting vulnerability exists due to a failure of the application to properly sanitize URI input prior to including it in dynamic content. An attacker may leverage this issue to have arbitrary script code executed in the browser of an unsuspecting user in the context of the Web administration page. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	ZyXEL B-240 Wireless Ethernet Adapter Web Interface Vulnerability	High	SecurityFocus, Bugtraq ID 12142, December 31, 2004

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Exploit name	Workaround or Patch Available	Script Description
January 2, 2005	viewcvs.txt	No	Exploit for ViewCVS 0.9.2 cross site scripting and HTTP-response splitting flaws.
January 2, 2005	sugarCRM.txt	No	Exploit for cross site scripting and possible code execution vulnerabilities in SugarCRM versions 1.x.
January 2, 2005	OWL-Intranet.txt	No	Exploit for OWL versions 0.7 and 0.8 cross site scripting and SQL injection vulnerabilities.
January 2, 2005	wins.c	Yes	Exploit for Remote Microsoft Windows 2000 WINS exploit that has connectback shellcode. Works on SP3/SP4.
January 2, 2005	HOD-ms04031-netdde-expl.c	Yes	Remote proof of concept exploit for the NetDDE buffer overflow vulnerability as described in MS04-031. Tested on: Windows XP Professional SP0, Windows XP Professional SP1, Windows 2000 Professional SP2, Windows 2000 Professional SP3, Windows 2000 Professional SP4, Windows 2000 Advanced Server SP4.

January 2, 2005	KorWeblog.txt	No	Exploit for KorWeblog directory traversal vulnerability that enables malicious attackers to access files and include malicious php files. Versions 1.6.2-cvs and below are susceptible.
January 2, 2005	ftpd-iexpl.c	No	Proof of concept exploit for Internet Explorer version 6.0.3790.0 that demonstrates an FTP download path disclosure flaw.
January 2, 2005	isec-0020-mozilla.txt	Yes	Exploit for a heap overflow vulnerability in Mozilla browser versions 1.7.3 and below in the NNTP code that may allow for arbitrary code execution.
January 2, 2005	phpcalendar.txt	No	Exploit for PHP-Calendar file inclusion vulnerability.
January 2, 2005	WHM-autopilot.txt	Yes	Exploit for WHM AutoPilot version 2.4.6.5 information disclosure, cross site scripting, and file inclusion vulnerabilities.
January 2, 2005	moodle142.txt	Yes	Exploit for Moodle versions 1.4.2 and below cross site scripting and file inclusion vulnerabilities.
January 2, 2005	netcat-exp.txt	Yes	Exploit for buffer overflow in netcat.
January 2, 2005	CMDExe.txt	Yes	Exploit for Internet Explorer remote command execution that is a variant of the Auto SP2 RC exploit.
January 2, 2005	ANI-DoS.txt	No	Exploit for Microsoft Windows Kernel ANI file parsing denial of service vulnerability.
January 2, 2005	PhpIncludeWorm.txt	No	PHP based worm that targets any vulnerable page or script with a remote file inclusion vulnerability.
January 2, 2005	SantyB.php.txt	No	Santy.b phpBB worm that affects versions 2.0.10 and below and installs a bot. Uses AOL/Yahoo search.
January 1, 2005	MSXPSP2-ieEXP.txt	No	Exploit for Internet Explorer HTML Help Control Local Zone bypass that can be used against Microsoft Windows XP versions SP2 and below.
January 1, 2005	yacyXSS.txt	Yes	Exploit for yacy version 0.31 cross site scripting attack vulnerability.
December 31, 2005	raptor_udf.c	No	Local root exploit that makes use of the dynamic library for do_system() in MySQL UDF. Tested on MySQL 4.0.17.
December 31, 2005	bruteforce.webmin.txt	Yes	Exploit for Webmin remote bruteforce and command execution.
December 31, 2005	exploitphpbb.zip	No	Perl script exploit extracted from the phpBB worm.
December 31, 2005	ibod_bof.c	No	Proof of concept buffer overflow exploit for IBOD 1.5.0 and below.
December 31, 2005	eboard40.txt	No	Exploit for e_Board version 4.0 directory traversal attack vulnerability.
December 31, 2005	cuteftpexpl.c	No	Exploit for CuteFTP Professional version 6.0 local denial of service vulnerability.
December 31, 2005	hijack_apache-0.1a.tar.gz	Yes	Tool to hijack HTTP connections under Apache and Apache2 with mod_php.
December 31, 2005	2bgalSQL.txt	No	Exploit for 2Bgal 2.5.1 SQL injection vulnerability.
December 31, 2005	php-openlog.txt	No	Proof of concept exploit for the PHP openlog() vulnerability inherent in PHP 4.3.x.
December 31, 2005	angelDust.c	Yes	Exploit for Snort 2.2.10 and below remote denial of service vulnerability.
December 31, 2005	e107.pl.txt	No	Remote exploit e107 input validation vulnerability.
December 31, 2005	pmc.pl.txt	No	Remote exploit for phpMyChat 0.14.5 that adds an administrative account.
December 31, 2005	raptor_chown.c	Yes	Local exploit for a flaw in Linux kernel that allows for group ownership change and possible system compromise. Tested against Linux kernel versions 2.4.x through 2.4.27-rc3 and 2.6.x through 2.6.7-rc3.
December 31, 2005	raptor_ldpreload.c	No	Local root exploit for a stack-based buffer overflow in the runtime linker, ld.so.1, on Solaris 2.6 through 9.
December 31, 2005	raptor_libdthelp.c	No	Local root exploit for a buffer overflow in CDE libDtHelp library.
December 31, 2005	raptor_libdthelp2.c	No	Local root exploit for a buffer overflow in CDE libDtHelp library.
December 31, 2005	raptor_passwd.c	No	Local root exploit for a vulnerability in the passwd circ() function under Solaris/SPARC 8/9.
December 31, 2005	raptor_rlogin.c	No	Remote root exploit for rlogin on Solaris/SPARC 2.5.1/2.6/7/8.
December 31, 2005	phpbbworm2.tgz	No	New version of the phpBB worm that successfully works against a patched phpBB 2.0.11.
December 31, 2005	SSA-20041220-16.txt	No	Exploit for input validation flaw in ZeroBoard versions 4.1pl4 and below.
December 31, 2005	phpbb-url.pl	N/A	Simple tool to automate the creation of the URL needed to exploit phpBB versions below 2.0.11 using the viewtopic.php vulnerability.
December 31, 2005	shoutcast194.c	No	Exploit for SHOUTcast DNAS/Linux version 1.9.4 format string vulnerability.
December 31, 2005	WPkontakt.txt	Yes	Exploit for WPKontakt versions 3.0.1 and below parsing error.
December 31, 2005	crystalPoC.c	No	Proof of concept exploit for Crystal FTP Pro version 2.8 flaw in the LIST command.
December 30, 2005	lsmcode.txt	Yes	Local root command execution exploit for lsmcode on AIX 5.1 to 5.3.
December 30, 2005	paginit.c	Yes	Local stack overflow exploit for /usr/bin/paginit on AIX versions 5.3/5.2/5.1.
December 30, 2004	ultrix_dxterm_4.5_exploit.c	No	Exploit for Ultrix 4.5/MIPS dxterm local root vulnerability.
December 30, 2004	ubbXSS.txt	No	Exploit for the cross site scripting vulnerabilities in the UBBThreads versions 6.2.3 and 6.5.
December 30, 2004	sugarSales.txt	No	Exploit for multiple vulnerabilities in the open source customer relationship management software SugarSales. These vulnerabilities include full path disclosure, file inclusion, remote command execution, and SQL injection attacks.
December 30, 2004	lithsock.zip	No	Remote denial of service proof of concept exploit for the Lithtech game engine that is susceptible to a denial of service.
December 30, 2004	isec-0018-igmp.txt	Yes	Exploit for local and remote vulnerabilities in the Linux IGMP networking module and the corresponding user API. Linux kernels 2.4 up to and include 2.4.28 and 2.6 up to and including 2.6.9 are affected.
December 30, 2004	isec-0019-scm.txt	Yes	Exploit for flaw in the Linux socket layer that allows a local user to hang a vulnerable machine. Kernel version 2.4 up to and including 2.4.28 and 2.6 up to and including 2.6.9 are susceptible.
December 30, 2004	firstclass.txt	Yes	OpenText FirstClass version 8.0 httpd /Search remote denial of service exploit.

December 30, 2004	phpGroupWare.txt	No	Exploit for phpGroupWare version 0.9.16.003 full path disclosure, cross site scripting, and SQL injection attacks.
December 30, 2004	aspSQL.txt	No	Exploit for asp-rider SQL injection attack vulnerability.
December 30, 2004	SSA-20041214-14.txt	Yes	Exploit for GNUBoard versions 3.39 and below suffer PHP injection vulnerability that allows for arbitrary command execution.
December 30, 2004	iwebnegar.txt	No	Exploit for SQL injection attack vulnerability in iwebnegar, the farsi weblog software.
December 30, 2004	wgettrap.txt	No	Proof of concept exploit for the wget directory traversal vulnerability that affects versions 1.8 and below.
December 30, 2004	rpcl_icmpdos.c	No	Exploit for RICOH Aficio 450/455 PCL 5e printer ICMP remote denial of service vulnerability.
December 30, 2004	un-aftpd.c	No	Exploit for Ability ftpd version 2.34 remote root vulnerability.
December 30, 2004	winrar341.txt	No	WinRAR proof of concept buffer overflow exploit for version 3.41 and below.
December 30, 2004	cscopesym.c	Yes	Local symlink exploit for cscope versions 15.5 and below.
December 30, 2004	kayako.txt	Yes	Exploit for Kayako eSupport version 2.x cross site scripting and SQL injection flaws.
December 25, 2004	phpbb_urldecode_poc.pl	No	Exploit for the PHPBB Remote URLDecode Input Validation vulnerability.

[back to top]

Trends

- **Poll: IT spending expected to fall.** IT spending in 2005 is expected to fall somewhat according to a new poll from CIO magazine. However, there are certain sectors, including security and storage, that are reportedly expected to rise. Only 6.7 percent of poll respondents indicated that they expected IT spending to increase in 2005, which was a decline of 1.7 percent from the poll's November results (8.4 percent). IT security spending is on the upswing with 60.9 percent of poll respondents indicating that they were planning on increasing spending over the next 12 months. The expected growth in security spending represents a 7.7 percent increase over November expectations (53.2 percent). A number of different studies in 2004 painted a very vivid picture of enterprises' attitudes toward IT security spending. A September Ernst & Young report noted that only 17 percent said spending would increase significantly, and 52 percent thought it would increase only slightly. In July, research firm IDC reported that 59 percent of its survey base indicated that IT security spending would increase. For more information: http://www.internetnews.com/stats/article.php/3453831
- **Suspicious probes target WINS servers.** The Bethesda, Md.-based SANS Internet Storm Center (ISC) said it and other organizations have seen a sharp uptick in probes against WINS servers since December 31. An attacker who successfully exploits the flaws in unpatched machines could take over the system to install programs; view, change or delete data; or create new accounts with full privileges. Microsoft issued fixes for the WINS security holes last month. Microsoft offered potential workarounds for those who are unable to patch systems immediately: Users can block TCP port 42 and UDP port 42 at the firewall or remove WINS altogether if it isn't needed. For more information: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1041758,00.html

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trends	Date
1	Netsky-P	Win32 Worm	Stable	March 2004
2	Sober-I	Win32 Worm	Stable	November 2004
3	Zafi-B	Win32 Worm	Stable	June 2004
4	Bagle-AU	Win32 Worm	Increase	October 2004
5	Bagle-AA	Win32 Worm	Increase	April 2004
6	Netsky-D	Win32 Worm	Decrease	March 2004
7	Netsky-Q	Win32 Worm	Slight Decrease	March 2004
8	Bagle.AT	Win32 Worm	Stable	October 2004
9	Netsky-Z	Win32 Worm	Decrease	April 2004
10	Bagle.BB	Win32 Worm	New to Table	September 2004

Table Updated January 4, 2005

Viruses or Trojans Considered to be a High Level of Threat

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Computer Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type
Asan.A	Net-Worm.Perl.Asan.a Perl/Asan.A.worm	Perl Worm
Backdoor.Lifefournow	Trojan-Proxy.Win32.Agent.l	Trojan
Backdoor.Ranky.P		Trojan
Backdoor.Sdbot.AI		Trojan
Backdoor.Zins		Trojan
Breacuk.E	W32/Breacuk.E.worm	Win32 Worm
Cabir.J	EPOC/Cabir.J SymbOS/Cabir.h SymbOS/Cabir.i SymbOS/Cabir.j SymbOS/Cabir.k Worm.Symbian.Cabir.J	Symbian OS Worm
Cabir.K	EPOC/Cabir.K SymbOS/Cabir.K Worm.Symbian.Cabir.K	Symbian OS Worm
Cabir.L	EPOC/Cabir.L SymbOS/Cabir.L Worm.Symbian.Cabir.L	Symbian OS Worm
Cabir.M	EPOC/Cabir.M SymbOS/Cabir.M Worm.Symbian.Cabir.M	Symbian OS Worm
Perl/Spyski.worm		Perl Worm
PERL_SANTY.C		Perl Worm
PWS-Banker!pwdrar		Trojan: Password Stealer
Skulls.D	SymbOS/Skulls.D	Symbian OS Worm
SYMBOS_VLASCO.A		Symbian OS Worm
Troj/Agent-FO	Trojan-Downloader.Win32.Agent.fo	Trojan
Troj/Bancban-AV	Trojan-Spy.Win32.Banker.fo	Trojan
Troj/BeastDo-W		Trojan
Troj/Chum-A	BackDoor-AZV.gen	Trojan
Troj/Santabot-A	BackDoor-AZV BackDoor-AZV.gen	Trojan
TROJ_BRDUPDATE.E		Trojan
Trojan.Kility		Trojan
W32.Cellery	Worm.Win32.VB.n Worm/Cellery Worm/VB.3.E WORM_CELLERY.A	Win32 Worm
W32.Protoride.B		Win32 Worm
W32/Dedler-H	Worm.Win32.Dedler Win32/Dedler.A WORM_ICQ.A	Win32 Worm
W32/Forbot-DH	Backdoor.Win32.Wootbot.gen	Win32 Worm
W32/Forbot-DJ	WORM_WOOTBOT.ES Backdoor.Win32.Wootbot.gen	Win32 Worm
W32/Gaobot.worm.gen.t		Win32 Worm
W32/Hilin.worm	Trojan-Spy.Win32.VB.dz W32/SillyFDC	Win32 Worm
W32/Kipis.b@MM	Email-Worm.Win32.Kipis.b Kipis.B	Win32 Worm
W32/Leebad-B	Worm.Win32.Leebad.c W32/Sautor.worm BKDR_SMALL.AE	Win32 Worm
W32/Puce-B		Win32 Worm
W32/RAHack	Backdoor-CMM W32.RAHack	Win32 Worm
W32/Sdbot.worm.gen.y		Win32 Worm
W32/Sdbot.worm.gen.z		Win32 Worm
W32/Sdbot-SV	WORM_SDBOT.AHR	Win32 Worm
W32/Sdbot-SW		Win32 Worm
Win32.Agobot.AMT	Backdoor.Win32.Agobot.wn W32.HLLW.Gaobot.gen W32/Agobot-OM W32/Gaobot.worm.gen.j	Win32 Worm

	Win32/Agobot.100352.A.Worm WORM_AGOBOT.ACZ	
Win32.Lospad.A	Dialer-234 Trojan.Win32.Dialer.bk Win32/Lospad.B.Trojan	Win32 Worm
Win32.Lospad.B	Dialer-234 Trojan.Win32.Dialer.bk Win32/Lospad.B.Trojan	Win32 Worm
Win32.SillyDl.BT	Downloader-PS TrojanDownloader.Win32.Small.vq Win32/SillyDl.AE.Trojan	Win32 Worm

[back to top]

Last updated January 05, 2005